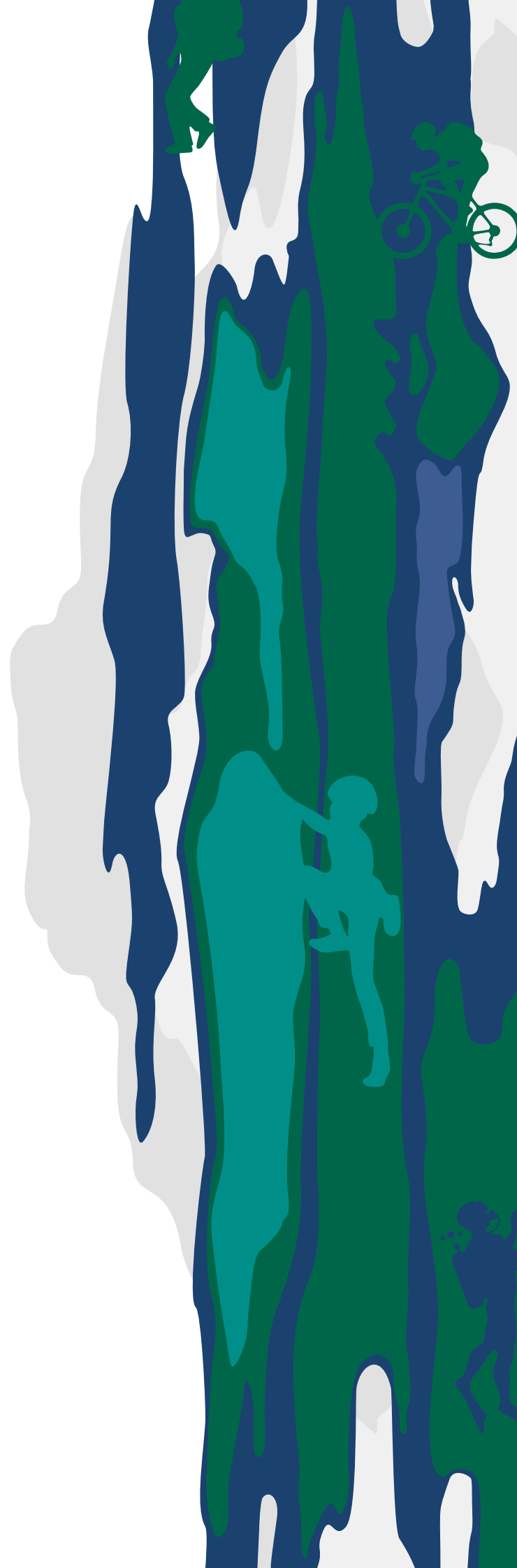




Scouts
AUSTRALIA

Digital Transformation RACI Matrix 2026



RACI - SCOUTS AUSTRALIA – NATIONAL DIGITAL SYSTEMS

RACI Legend

- R** Responsible Performs the activity or delivers the work.
- A** Accountable Ultimately answerable for the activity and decision-making authority. Only one Accountable role per activity.
- C** Consulted Provides input or subject matter expertise prior to a decision.
- I** Informed Kept up to date on progress or outcomes.

Digital Activity	National Executive Committee (NEC)	BCMSC	National Commissioners	National Office (NST)	National Operations Committee (NOC)	National Executive Officers Network (NEON)	Branch Board / Exec Committee (BECs)	Branch IT Teams
Digital strategy & roadmap	A	R	C	C	C	C	C	I
Enterprise architecture & standards	C	I	C	A/ R	C	C	C	I
Technology stack approval	C	C	C	A/ R	C	C	C	I
National system ownership	A	C	I	R	C	I	I	C
System selection & approval	A	C	C	R	C	C	C	C
System implementation (national)	C	C	C	A/ R	C	C	I	I
Data governance framework	A	C	I	R	C	I	C	I
Privacy & regulatory compliance (Australia)	A	C	C	R	C	C	C	I
Cyber security standards (Essential Eight)	A			R			C	I
Cyber / data incident response	C	I	I	A/ R	I	I	I	I
Identity & access management	C		I	A/ R	I	I	C	R (Local Triggers)
User support – Tier 1	C		I	A/ R	I	I	I	R
User support – Tier 2/3	C		I	A/ R	I	I	I	C

Digital Activity	National Executive Committee (NEC)	BCMSC	National Commissioners	National Office (NST)	National Operations Committee (NOC)	National Executive Officers Network (NEON)	Branch Board / Exec Committee (BECs)	Branch IT Teams
User training & adoption	I	C	C	A/ R	C	C	C	C
Vendor panels & contracts	A	C	I	R	C	C	I	I
Vendor performance management	I	C	I	A/ R	C	C	I	I
Digital investment prioritisation	A	C	C	R	C	C	C	I
Funding – national systems	A	C	C	R	C	C	I	I
Change management framework	A		C	R	C	C	C	I
Major digital change approvals	A	C	C	R	C	C	C	I
Digital risk framework	A	C	C	R	C	C	C	I
Determination of business requirements	A	R	R	R	C	C	I	I
Standard Operating Procedures in place and current	I		C	A/ R	C	C		C

DIGITAL ACTIVITY COMPONENTS – EXPLANATIONS

Note: Branch-only / owned systems are excluded from this RACI

Ownership of systems used exclusively within a Branch, including funding, maintenance, compliance, and support. These systems fall under the RACI model held by each Branch and are out of scope for a National Digital System RACI. However, any Data Sharing Agreements between a Branch and Scouts Australia remain in place.

Digital strategy and roadmap

A long-term plan that sets the direction, priorities, and sequencing for digital systems, technology investments, and capability development across the organisation.

Enterprise architecture and standards

The organisation-wide blueprint for how systems, data, integrations, and technologies fit together, including the rules, patterns, and standards that guide digital design and interoperability.

Technology stack approval

The process of selecting and approving the major technology components used across the organisation to ensure consistency and supportability.

National system ownership

Formal accountability for national-level digital systems, including governance, performance, compliance, and lifecycle management.

System selection and approval

The process of evaluating options, conducting due diligence, and approving which digital system is chosen for a particular business need. The Scouts Australia Digital Member Experience Principles and the Digital System Design Principles must be applied in the assessment and selection process.

System implementation (national)

Delivery of national digital systems from design through deployment, including configuration, testing, training, and go-live.

Data governance framework

The policies, rules, and structures that ensure data is accurate, protected, safely used, and managed consistently across the organisation.

Privacy and regulatory compliance (Australia)

Ensuring all systems and processes comply with relevant national and state privacy, data protection, and digital regulatory requirements.

Cyber security standards (Essential Eight)

Application of the Australian Signals Directorate's Essential Eight maturity model or similar baseline controls to minimise cyber risks.

Cyber / data incident response

Cyber / data incident response

The process for detecting, reporting, managing, and resolving cyber security incidents or data breaches, including required notifications.

Identity and access management

Systems and processes that ensure the right people have the right access to the right systems at the right time.

User support – Tier 1

Front-line user support that logs issues, resolves simple problems, and triages more complex matters.

User support – Tier 2/3

More specialised technical support that resolves complex system issues, escalating to vendors or system experts where required.

User training and adoption

Activities that help volunteers and staff understand, learn, and effectively use systems.

Vendor panels and contracts

Management of approved digital suppliers, including procurement processes, contract negotiation, and compliance with procurement rules.

Vendor performance management

Ongoing monitoring of vendor delivery against service levels, contracts, and performance expectations.

Digital investment prioritisation

Assessment and ranking of digital proposals so that funding and resources go to the most important initiatives based on business value and risk.

Funding – national systems

Budgeting and financial oversight for digital systems operated at a national level.

Change management framework

A structured approach for planning, approving, and managing changes to digital systems, processes, and user behaviour.

Major digital change approvals

Governance processes that approve significant system changes, upgrades, or new digital initiatives before they proceed.

Digital risk framework

The policies, tools, and processes used to identify, assess, monitor, and mitigate digital and cyber risks at an organisational level.

Determination of Business Requirements

Determination of business requirements refers to the structured process of identifying, analysing, documenting, and validating the needs and objectives of the business to support a specific initiative, project, or operational activity. This includes engaging relevant stakeholders, capturing functional and non-functional requirements, prioritizing needs, and ensuring alignment with strategic goals.

Standard Operating Procedures in place and current

Standard Operating Procedures (SOPs) are formally documented, approved, and accessible processes that describe how key activities are to be performed. These SOPs are regularly reviewed, updated, and version-controlled to ensure they remain accurate, relevant, and aligned with current business practices, regulatory requirements, and organizational objectives.